SecurityScorecard

INFORME DETALLADO

Scorecard para Alliance Enterprise

Generado **11 de octubre de 2023**
por Fredy Sanchez (fredy.sanchez@bancounion.com), Banco Union

Acerca de este informe
Este informe es una captura puntual de este Scorecard desde las 19:58:31 UTC del 11 de octubre de 2023. No debe confundirse con un resultado de prueba de penetración ni con una evaluación final.

Obtenga una visión global con SecurityScorecard
SecurityScorecard ofrece control automático continuo, informes de historial, exportaciones de datos en formato CSV y muchas más funciones que ayudarán a los equipos de seguridad a proteger sus organizaciones. Para obtener acceso gratuito al Scorecard de su organización, cree una cuenta hoy mismo en bit.ly/2P8okyb.

Obtenga hoy mismo más información sobre SecurityScorecard en bit.ly/2xXNg4N.

¿Qué es SecurityScorecard?
SecurityScorecard es un servicio de calificación (Score) de seguridad que utiliza un sencillo sistema de calificación de la A (puntuación máxima) a la F (puntuación mínima) para calificar la seguridad general de las empresas, así como 10 importantes factores de riesgo. Una empresa con una calificación C, D o F tiene 5,4 veces más probabilidades de sufrir una filtración importante que empresas con una calificación A o B1. Ciertos factores de riesgo, como la seguridad de las aplicaciones y la cadencia de la aplicación de revisiones, tienen aún más efecto sobre la probabilidad de sufrir una filtración. Si se obtiene una F en lugar de una A en dichos factores, la probabilidad de que se produzca una filtración de datos o un ataque es diez veces mayor.

Obtenga más información sobre el sistema de Score de SecurityScorecard en bit.ly/2zMLSmW.

1 "La investigación de SecurityScorecard puede ayudarle a detectar una fuga de datos antes de que esta ocurra" (https://bit.ly/2yc0JVN)

Próximos pasos: Permanecer en (A)

1. Cree una cuenta
Este archivo incluye muchos detalles, pero recuerde: se refiere solo a un momento puntual. Cree una cuenta si quiere obtener acceso completo y gratuito al Scorecard completo de su organización, además de auto-monitoreo continuo, informes de historial, exportaciones de datos en formato CSV y otras muchas cosas.

2. Valide su huella digital
Una vez que tenga una cuenta, revise la huella digital de su empresa, los activos que SecurityScorecard considera potencialmente atribuibles a su empresa, que afectan a las calificaciones de su Scorecard. Solicite la eliminación o adición de IP según sea necesario.

3. Examine los hallazgos sobre los problemas
Investigue junto con sus equipos el contenido de su tarjeta de puntuación. La postura de seguridad de su empresa saldrá ganando si se identifican cabos sueltos de los que antes no eran conscientes.

4. Detecte nuevos problemas, manténgase en (A)
Tanto si ha aplicado una corrección como si ha encontrado activos que no pertenecen a su empresa o desea compartir información sobre los controles de compensación, puede informarnos solucionando los problemas identificados y enviándolos para que aprobemos su resolución. Nuestro equipo de suporte se encarga de gestionar las resoluciones y resolverá cualquier asunto pendiente en un plazo de tres días hábiles. Corrija los problemas en la propia plataforma o envíe un correo electrónico a support@securityscorecard.com.

Estamos aquí para ayudarle

La plataforma SecurityScorecard se basa en la transparencia y la colaboración. Nuestro equipo de Asistencia para fiabilidad del cliente proporciona servicios de corrección y resolución sin cargo alguno y estaremos encantados de trabajar con usted y sus clientes para resolver cualquier problema. Si necesita ayuda en cualquier momento, contacte con nosotros enviando un correo electrónico a support@securityscorecard.io.

Visión general del Scorecard

A

Alliance Enterprise

Puntuación de seguridad: 91

DOMINIO: allianceenterprise.com

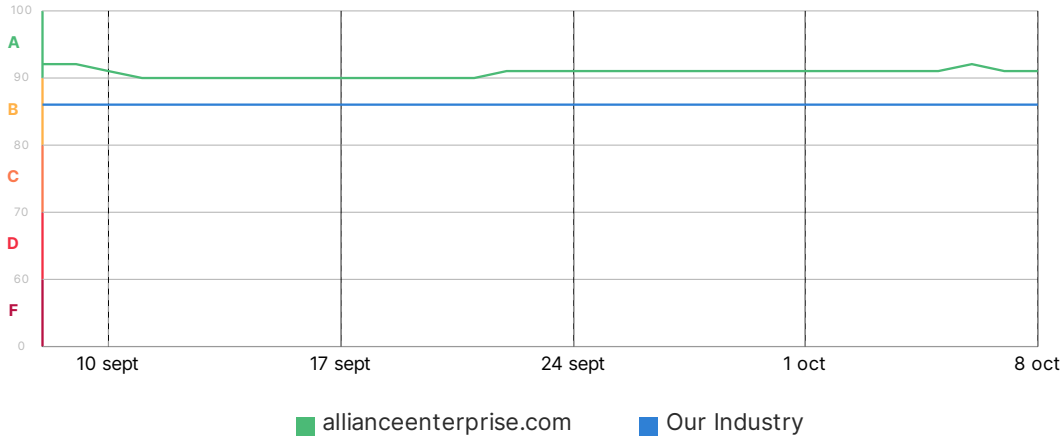
SECTOR: SERVICIOS DE INFORMACIÓN

Factores de Riesgo

C	75	SEGURIDAD DE APLICACIÓN WEB	6 INCIDENCIAS		
A	100	CUBIT SCORE	0 NINGUNA INCIDENCIA		
A	100	ESTADO DE DNS	0 NINGUNA INCIDENCIA		
A	100	SEGURIDAD DE PUNTOS DE CONEXIÓN	0 NINGUNA INCIDENCIA		
A	100	HACKER CHATTER	0 NINGUNA INCIDENCIA		
A	100	REPUTACIÓN DE IP	0 NINGUNA INCIDENCIA		
A	100	FILTRACIÓN DE INFORMACIÓN	0 NINGUNA INCIDENCIA		
C	79	SEGURIDAD DE RED	4 INCIDENCIAS		
A	100	CADENCIA DE APLICACIÓN DE REVISIONES	0 NINGUNA INCIDENCIA		
A	100	INGENIERÍA SOCIAL	0 NINGUNA INCIDENCIA		

Historial del Score en los últimos 30 días

En el siguiente cuadro se muestra la evolución de la clasificación de seguridad relativa de la empresa a lo largo del tiempo. Los picos en la puntuación de rendimiento representan mejoras en la seguridad general, corrección de incidencias abiertas y mejoras en la protección de la infraestructura de la empresa. Las caídas reflejan la introducción de configuraciones erróneas en el sistema o la aplicación, o bien actividades prolongadas de malware.



Elementos de acción

FACTOR	GRAVEDAD	IMPACTO EN EL SCORE	PROBLEMAS DETECTADOS
Seguridad de aplicación web	!!	-1.8	Falta la política de seguridad de contenido (PSC). Una política de seguridad de contenido (PSC) indica a un navegador web desde qué ubicaciones puede cargar recursos al renderizar una página web. Esto ayuda a evitar la inyección de recursos erróneos o malintencionados en una página web (y su posterior ejecución por parte del navegador de un usuario).
	!!	-1.1	Patrón de redireccionamiento HTTPS inseguro. El sitio redirige a un dominio de forma que limita la seguridad proporcionada por los encabezados HTTPS y HTTP Strict Transport Security (HSTS), creando una vulnerabilidad mediante la cual los usuarios acaban redirigidos a una versión falsificada/malintencionada del sitio.
	!!	-1.1	La cadena de redireccionamiento contiene HTTP. El sitio redirige a través de URL que no están protegidas con HTTPS; esto deja a los usuarios vulnerables frente a redirecciones a una versión falsificada/malintencionada del sitio de destino.
	!!	-1.9	El sitio web no implementa las prácticas recomendadas de HSTS. Incluso si un sitio web está protegido con HTTPS, la mayoría de los navegadores intentarán conectarse primero a la versión HTTP del sitio web a menos que se especifique explícitamente. En ese momento, los visitantes del sitio web son vulnerables a un atacante de tipo “man in the middle” que puede impedirles llegar a la versión HTTPS del sitio web que pretendían visitar y, en su lugar, desviarlos a un sitio web malintencionado. El encabezado HSTS (expand) garantiza que, después de la visita inicial de un usuario al sitio web, no sean susceptibles a este ataque de intermediario, porque se conectarán inmediatamente al sitio web protegido por HTTPS.
	!	-0.5	El sitio no aplica las prácticas recomendadas para evitar la incrustación de contenido malintencionado. Hemos observado que el sitio web de esta organización no aplica las prácticas recomendadas para evitar que los atacantes incrusten su contenido en un marco en sitios web no fiables o malintencionados. Los atacantes pueden aprovecharse escenificando ataques de secuestro de clic, que consisten en engañar a los visitantes del sitio web para que hagan clic en objetos malintencionados que provocan la revelación de información confidencial. Por ejemplo, si una página tiene los clics secuestrados y un usuario hace clic en "Me gusta", puede comprometer su navegador u ordenador.
	!	-0.5	El sitio web no implementa las prácticas recomendadas de X-Content-Type-Options. A veces los navegadores analizan el contenido por sí mismos y lo manejan según el encabezado de tipo MIME; esto puede ocasionar problemas de seguridad y ejecución de código malintencionado. Por ejemplo, un atacante podría ocultar código malintencionado con una extensión de imagen, que el navegador analizaría y ejecutaría como JavaScript.
Seguridad de red	!!!	-1.7	El servicio SSL/TLS admite un protocolo débil. Se ha observado que un servicio TLS admitía protocolos débiles.
	!!	-1.2	El certificado es autofirmado. Los certificados autofirmados impiden que los clientes TLS se conecten a los servidores.
	!	-0.5	La vida útil del certificado es más larga de lo que las prácticas recomendadas aconsejan. Se ha observado que el periodo de validez de un certificado era más largo que el dictado por los requisitos de referencia del foro CAB.
	!	-0.5	Certificado sin control de revocación. Se ha observado que un certificado no contenía URL de CRL ni OCSP.

C 75 SEGURIDAD DE APLICACIÓN WEB

El módulo Seguridad de aplicación web utiliza inteligencia sobre amenazas entrantes por vulnerabilidades conocidas, que se identifican mediante bases de datos CVE “whitehat”, bases de datos de vulnerabilidades “blackhat” y hallazgos importantes indexados por los principales motores de búsqueda. El módulo se nutre de datos de varios conjuntos de datos públicos, fuentes de terceros y un motor interno de indexación y agregación patentado.
La puntuación determina la probabilidad de una próxima filtración en la aplicación web y comprueba si hay algún código de "defacement" (desfiguración) existente. La presencia de aplicaciones vulnerables, versiones obsoletas y desfiguraciones activas se utiliza para calcular la puntuación general.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Application Security

GRAVEDAD MEDIA

Falta la política de seguridad de contenido (PSC)	2
Patrón de redireccionamiento HTTPS inseguro	1
La cadena de redireccionamiento contiene HTTP	1
El sitio web no implementa las prácticas recomendadas de HSTS	2

GRAVEDAD BAJA

El sitio no aplica las prácticas recomendadas para evitar la incrustación de contenido malintencionado	2
El sitio web no implementa las prácticas recomendadas de X-Content-Type-Options	2

POSITIVA

No hay Señales positivos para Application Security

INFORMATIVOS

No hay Señales informativos para Application Security

Falta la política de seguridad de contenido (PSC)

-1.8 IMPACTO EN EL SCORE

Una política de seguridad de contenido (PSC) indica a un navegador web desde qué ubicaciones puede cargar recursos al renderizar una página web.
Esto ayuda a evitar la inyección de recursos erróneos o malintencionados en una página web (y su posterior ejecución por parte del navegador de un usuario).

Descripción

La política de seguridad de contenido proporciona una valiosa red de seguridad que protege su sitio web frente a ataques malintencionados de scripts de sitios (XSS).
Una política bien configurada impedirá que un atacante trate de insertar en su sitio web su código o referencias a otro contenido malintencionado.
Sin una política de seguridad de contenido, es fácil que los desarrolladores de sitios web cometan errores que permitan a un atacante inyectar contenido que cambie la forma en que el sitio web se comporta.

Recomendación

Habilite los encabezados PSC mediante la configuración de su servidor web.

2 resultados

DOMINIO	ESQUEMA	OBSERVACIONES	URL FINAL	FECHA DE ÚLTIMA OBSERVACIÓN
allianceenterprise.com	https	9	https://ftp.allianceenterprise.com/	8/10/2023 2:31:09
allianceenterprise.com	https	911	https://allianceenterprise.com/	4/10/2023 18:56:16

El sitio no aplica las prácticas recomendadas para evitar la incrustación de contenido malintencionado

-0.5 IMPACTO EN EL SCORE

Hemos observado que el sitio web de esta organización no aplica las prácticas recomendadas para evitar que los atacantes incrusten su contenido en un marco en sitios web no fiables o malintencionados. Los atacantes pueden aprovecharse escenificando ataques de secuestro de

clic, que consisten en engañar a los visitantes del sitio web para que hagan clic en objetos malintencionados que provocan la revelación de información confidencial. Por ejemplo, si una página tiene los clics secuestrados y un usuario hace clic en "Me gusta", puede comprometer su navegador u ordenador.

Descripción
Una práctica recomendada para evitar la incrustación malintencionada de contenido del sitio es añadir la directiva de ancestros de marcos (frame-ancestors) al encabezado de respuesta HTTP de la política de seguridad de contenido (CSP) del sitio. Esta directiva limita qué URL puede incrustar contenido del sitio mediante elementos HTML como <frame>, <iframe>, <object>, <embed> o <applet>. Usar un encabezado CSP con la directiva de ancestros de marcos es preferible a usar las opciones de X-Frame (X-Frame-Options), que no admiten todos los navegadores. La especificación CSP es compatible con la mayoría de los navegadores modernos y ofrece compatibilidad retroactiva para los navegadores más antiguos. Si el encabezado de respuesta HTTP incluye tanto las X-Frame-Options como los ancestros de marcos, los navegadores ignorarán las X-Frame-Options por considerarlas obsoletas.

Recomendación
Configure un encabezado de respuesta con ancestros de marcos mediante una lista <source> que especifique qué URL pueden incrustar los elementos del sitio. O bien, utilice la palabra clave "none" (ninguno) para que ningún URL pueda incrustar contenido del sitio. Otra opción es utilizar la palabra clave "self" (auto) para permitir la incrustación solamente al sitio que sirve el contenido.

2 resultados

ANÁLISIS	DOMINIO	ESQUEMA	OBSERVACIONES	URL FINAL	FECHA DE ÚLTIMA OBSERVACIÓN
frame_ancestors_missing	allianceenterprise.com	https	9	https://ftp.allianceenterprise.com/	8/10/2023 2:31:09
frame_ancestors_missing	allianceenterprise.com	https	175	https://allianceenterprise.com/	4/10/2023 18:56:16

Patrón de redireccionamiento HTTPS inseguro

-1.1 IMPACTO EN EL SCORE

El sitio redirige a un dominio de forma que limita la seguridad proporcionada por los encabezados HTTPS y HTTP Strict Transport Security (HSTS), creando una vulnerabilidad mediante la cual los usuarios acaban redirigidos a una versión falsificada/malintencionada del sitio.

Descripción
El sitio HTTP redirige a los usuarios a una nueva URL de una forma que no se puede proteger con encabezados HTTPS y HSTS. Esto deja a los usuarios expuestos a ataques de tipo “man in the middle” que pueden redirigirlos a una versión fraudulenta/falsificada del sitio. Consulte el tipo de problema “El sitio no aplica HTTPS” para obtener más información sobre los escenarios de ataques de tipo “man in the middle”.

Recomendación
Cualquier sitio HTTP debe redirigir al usuario a una versión segura (es decir, HTTPS) del mismo dominio que se solicitó originalmente (o a una versión de nivel superior/matriz de ese mismo dominio). Por ejemplo, http://www.ejemplo.com solo debe redirigirse a https://www.ejemplo.com o https://ejemplo.com. Este redireccionamiento debe realizarse antes de redirigir a cualquier otro dominio o subdominio.

1 resultado

ANÁLISIS	DOMINIO	ESQUEMA	OBSERVACIONES	URL FINAL	URL INICIAL	FECHA DE ÚLTIMA OBSERVACIÓN
https_redirect_missing_hsts_header	allianceenterprise.com	https	5	https://allianceenterprise.com/	http://www.allianceenterprise.com/	4/10/2023 18:56:16

Evidencias:

La cadena de redireccionamiento contiene HTTP

-1.1 IMPACTO EN EL SCORE

El sitio redirige a través de URL que no están protegidas con HTTPS; esto deja a los usuarios vulnerables frente a redirecciones a una versión falsificada/malintencionada del sitio de destino.

Descripción
Mientras se redirige a un usuario a su destino URL final, pasa a través de una o más URL servidas a través de HTTP (en lugar de HTTPS). Tener enlaces HTTP en una cadena de redireccionamiento debilita otras tecnologías de seguridad (por ejemplo, encabezados HTTPS y HSTS) que se implementan en otras partes de la cadena.

Recomendación
Cualquier sitio HTTP debe redirigir inmediatamente a los usuarios a URL protegidas por HTTPS y asegurarse de que no se produzcan más redireccionamientos a través de HTTP. Cuando esté disponible es preferible el uso de URL HTTPS en lugar de HTTP y evitar redireccionamientos innecesarios.

1 resultado

DOMINIO	ESQUEMA	OBSERVACIONES	URL FINAL	URL INICIAL	FECHA DE ÚLTIMA OBSERVACIÓN
allianceenterprise.com	https	3	https://allianceenterprise.com/	http://alliensoft.com/	2/10/2023 10:31:20
Evidencias:					

El sitio web no implementa las prácticas recomendadas de HSTS

-1.9 IMPACTO EN EL SCORE

Incluso si un sitio web está protegido con HTTPS, la mayoría de los navegadores intentarán conectarse primero a la versión HTTP del sitio web a menos que se especifique explícitamente. En ese momento, los visitantes del sitio web son vulnerables a un atacante de tipo “man in the middle” que puede impedirles llegar a la versión HTTPS del sitio web que pretendían visitar y, en su lugar, desviarlos a un sitio web malintencionado. El encabezado HSTS (expand) garantiza que, después de la visita inicial de un usuario al sitio web, no sean susceptibles a este ataque de intermediario, porque se conectarán inmediatamente al sitio web protegido por HTTPS.

Descripción
HTTP Strict Transport Security (HTTP con seguridad de transporte estricta) es un encabezado HTTP que indica a los clientes (por ejemplo, navegadores web) que solo se conecten a un sitio web mediante conexiones HTTPS cifradas. Los clientes que respeten este encabezado actualizarán automáticamente todos los intentos de conexión de HTTP a HTTPS.
Una vez que un cliente recibe el encabezado HSTS en su primera visita al sitio web, las conexiones futuras a ese sitio web están protegidas frente a ataques de tipo “man in the middle” que intentan la degradación a una conexión HTTP no cifrada.
El navegador dará por caducado el encabezado HTTP Strict Transport Security después del número de segundos configurado en el atributo de antigüedad máxima.

Recomendación
Toda aplicación web (y cualquier URL por la que se pase para llegar al sitio web mediante redireccionamientos) debe configurar el encabezado HSTS para que permanezca en vigor durante al menos 12 meses (31 536 000 segundos). Igualmente se recomienda configurar la directiva “includeSubDomains” para que las solicitudes a subdominios también se actualicen automáticamente a HTTPS.
Un encabezado HSTS aceptable sería:
Strict-Transport-Security: max-age=31536000; includeSubDomains;

2 resultados

ANÁLISIS	DOMINIO	ESQUEMA	OBSERVACIONES	URL FINAL	FECHA DE ÚLTIMA OBSERVACIÓN
no_hsts	allianceenterprise.com	https	909	https://allianceenterprise.com/	4/10/2023 18:56:16
no_hsts	allianceenterprise.com	https	9	https://ftp.allianceenterprise.com/	8/10/2023 2:31:09

El sitio web no implementa las prácticas recomendadas de X-Content-Type-Options

-0.5 IMPACTO EN EL SCORE

A veces los navegadores analizan el contenido por sí mismos y lo manejan según el encabezado de tipo MIME; esto puede ocasionar problemas de seguridad y ejecución de código malintencionado. Por ejemplo, un atacante podría ocultar código malintencionado con una extensión de imagen, que el navegador analizaría y ejecutaría como JavaScript.

Descripción

Un tipo MIME es un encabezado HTTP que indica el tipo de contenido devuelto en una respuesta y cómo debe manejarlo y mostrarlo el navegador.
A veces los navegadores analizan el contenido por sí mismos y lo manejan según el encabezado de tipo MIME; esto puede ocasionar problemas de seguridad y ejecución de código malintencionado.
El encabezado X-Content-Type-Options indica que los navegadores siempre deben confiar en el tipo MIME declarado desde el servidor y no intentar analizar el contenido por sí mismos.

Recomendación

Añada el siguiente encabezado a las respuestas de este sitio web: “X-Content-Type-Options: nosniff”

2 resultados

ANÁLISIS	DOMINIO	ESQUEMA	OBSERVACIONES	URL FINAL	FECHA DE ÚLTIMA OBSERVACIÓN
x_content_type_options_missing	allianceenterprise.com	https	9	https://ftp.allianceenterprise.com/	8/10/2023 2:31:09
x_content_type_options_missing	allianceenterprise.com	https	911	https://allianceenterprise.com/	4/10/2023 18:56:16

A 100 CUBIT SCORE

Este módulo patentado mide distintos problemas de seguridad que una empresa podría tener. Por ejemplo, comprobamos las bases de datos públicas sobre inteligencia de amenazas en busca de direcciones IP que hayan sido señaladas. Estas configuraciones erróneas pueden presentar una alta vulnerabilidad y podrían causar daños significativos a la privacidad de sus datos e infraestructura.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Cubit Score

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Cubit Score

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Cubit Score

POSITIVA

No hay Señales positivos para Cubit Score

INFORMATIVOS

No hay Señales informativos para Cubit Score

No se encontró ningún problema

A 100 ESTADO DE DNS

Este módulo mide el estado y la configuración de los ajustes DNS de una empresa. Verifica que no se hayan producido eventos maliciosos en el historial del DNS pasivo de la red de la empresa, ayuda a validar que los servidores de correo tengan la protección adecuada para evitar la falsificación (o "spoofing") y permite verificar que los servidores DNS estén configurados correctamente.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para DNS Health

GRAVEDAD MEDIA

No hay Problemas de gravedad media para DNS Health

GRAVEDAD BAJA

No hay Problemas de gravedad baja para DNS Health

POSITIVA

No hay Señales positivos para DNS Health

INFORMATIVOS

No hay Señales informativos para DNS Health

No se encontró ningún problema

A 100 SEGURIDAD DE PUNTOS DE CONEXIÓN

El módulo Seguridad de puntos de conexión realiza un seguimiento de los puntos de identificación que se extraen de metadatos relacionados con el sistema operativo, el navegador web y los complementos activos relacionados. La información recopilada permite a las empresas identificar versiones obsoletas de estos puntos de datos que pueden dar lugar a vulnerabilidad y ataques en el lado del cliente.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Endpoint Security

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Endpoint Security

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Endpoint Security

POSITIVA

No hay Señales positivos para Endpoint Security

INFORMATIVOS

No hay Señales informativos para Endpoint Security

No se encontró ningún problema

A 100 HACKER CHATTER

El módulo Hacker Chatter de SecurityScorecard es un sistema automatizado de recopilación y agregación para el análisis de múltiples flujos de charla de piratas informáticos en sitios clandestinos. Continuamente se supervisan, recopilan y agregan foros, IRC, redes sociales y otros repositorios públicos de conversaciones de la comunidad de piratas informáticos para localizar menciones a nombres de empresas y sitios web. La puntuación de Hacker Chatter es una clasificación informativa de indicadores basada en la cantidad de indicadores detectados por los sensores de recopilación.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Hacker Chatter

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Hacker Chatter

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Hacker Chatter

POSITIVA

No hay Señales positivos para Hacker Chatter

INFORMATIVOS

No hay Señales informativos para Hacker Chatter

No se encontró ningún problema

A 100 REPUTACIÓN DE IP

Los módulos Reputación de IP y Exposición al malware utilizan la infraestructura de sistemas “sinkhole” de SecurityScorecard, así como una combinación de fuentes de malware OSINT y asociaciones de intercambio de datos de inteligencia de amenazas de terceros. El sistema “sinkhole” de SecurityScorecard ingiere millones de señales de malware procedentes de infraestructuras de comando y control (C2) de todo el mundo. Los datos entrantes se procesan y atribuyen a las empresas. La cantidad y duración de las infecciones por malware se utilizan como factor determinante para calcular el indicador clave de amenaza del módulo Exposición al malware.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para IP Reputation

GRAVEDAD MEDIA

No hay Problemas de gravedad media para IP Reputation

GRAVEDAD BAJA

No hay Problemas de gravedad baja para IP Reputation

POSITIVA

No hay Señales positivos para IP Reputation

INFORMATIVOS

No hay Señales informativos para IP Reputation

No se encontró ningún problema

A 100 FILTRACIÓN DE INFORMACIÓN

Este módulo Filtración de información hace uso de las capacidades de supervisión de charlas y supervisión de la Deep Web para identificar las credenciales comprometidas que los piratas informáticos están haciendo circular. Se trata de filtraciones masivas de datos anunciadas públicamente, así como filtraciones e intercambios más pequeños entre piratas informáticos.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Information Leak

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Information Leak

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Information Leak

POSITIVA

No hay Señales positivos para Information Leak

INFORMATIVOS

No hay Señales informativos para Information Leak

No se encontró ningún problema

C 79 SEGURIDAD DE RED

El módulo Seguridad de red comprueba los conjuntos de datos públicos en busca de pruebas de puertos abiertos de alto riesgo o inseguros dentro de la red de la empresa. Los puertos inseguros a menudo se pueden explotar para permitir que un atacante eluda el proceso de inicio de sesión u obtenga un acceso profundo al sistema. Si está mal configurado, el puerto abierto puede actuar como punto de entrada entre la estación de trabajo de un pirata informático y su red interna.

GRAVEDAD ALTA		GRAVEDAD MEDIA		GRAVEDAD BAJA		POSITIVA
El servicio SSL/TLS admite un protocolo débil	1	El certificado es autofirmado	1	La vida útil del certificado es más larga de lo que las prácticas recomendadas aconsejan	2	No hay Señales positivos para Network Security
				Certificado sin control de revocación	2	**INFORMATIVOS**
						No hay Señales informativos para Network Security

La vida útil del certificado es más larga de lo que las prácticas recomendadas aconsejan

-0.5 IMPACTO EN EL SCORE

Se ha observado que el periodo de validez de un certificado era más largo que el dictado por los requisitos de referencia del foro CAB.

Descripción
Cuando una Entidad de certificación (CA) emite un certificado, incrusta dos fechas: la fecha en la que el certificado comienza a ser válido y la fecha en la que el certificado deja de ser válido.
Los algoritmos criptográficos no tienen una vida definida, pero académicos, investigadores y estados los evalúan constantemente en busca de puntos débiles. El foro CAB de entidades de certificación (CA) y navegadores, un grupo del sector que establece normas sobre la creación y el uso de certificados, publica periódicamente un documento conocido como los Requisitos de referencia (BR). Cada dos años aproximadamente, estos BR se actualizan para reducir el periodo máximo de validez de los certificados emitidos a partir de una fecha específica. Los certificados más antiguos tienen periodos de validez más largos, pero los emitidos después del 1 de septiembre de 2020 deben tener periodos de validez de 398 días como máximo.

Recomendación
Si el servicio no está en uso, desmantélelo. Si lo está, contacte con su CA y pida que emitan un nuevo certificado.

2 resultados

OBJETIVO	HUELLA DIGITAL SHA-256	OBSERVACIONES	SALIDA	FECHA DE ÚLTIMA OBSERVACIÓN
190.144.214.233	d5df1086ad1d754280aeb42016244b2d017eca143d6834281eeaa3cea85bdd7a02			6/10/2023 4:13:13
Evidencias:				
190.144.214.233	492daf7b137f54fcb0bdeaea7 5793a443a2e0a5a7bbcaee9bb3d405e92f21ee206	57		7/10/2023 8:28:30
Evidencias:				

El servicio SSL/TLS admite un protocolo débil

-1.7 IMPACTO EN EL SCORE

Se ha observado que un servicio TLS admitía protocolos débiles.

Descripción
La Seguridad de capa de transporte (TLS), protocolo sucesor de la Capa de sockets seguros (SSL), es un protocolo de red que cifra las comunicaciones entre los servidores TLS (por ejemplo, sitios web) y los clientes TLS (por ejemplo, navegadores web). Todas las comunicaciones están protegidas por un conjunto de cifrado: una combinación de varios algoritmos que trabajan en sintonía.
Los protocolos de red no tienen una vida definida, pero académicos, investigadores y estados los evalúan constantemente en busca de puntos débiles. El consenso sobre qué protocolos se consideran de poca confianza cambia con el tiempo y si las comunicaciones se envían con un protocolo débil, dicha comunicación puede alterarse o falsificarse.

Recomendación
Desactive los protocolos que figuran en la columna de evidencia de la medición.

1 resultado

OBJETIVO	PUERTO	OBSERVACIONES	FECHA DE ÚLTIMA OBSERVACIÓN
190.144.214.233	4433	17	7/10/2023 8:28:30

Certificado sin control de revocación

-0.5 IMPACTO EN EL SCORE

Se ha observado que un certificado no contenía URL de CRL ni OCSP.

Descripción
Cuando una Entidad de certificación (CA) emite un certificado, incrusta URL que se pueden visitar para comprobar si un certificado se ha revocado. Los certificados revocados ya no son válidos y los clientes de TLS (por ejemplo, los navegadores web) se negarán a conectarse a los servidores que presenten certificados revocados.
Los certificados se revocan por distintas razones: el desmantelamiento de un servidor, la retirada de un producto o nombre comercial, la renovación anticipada de un certificado o la sospecha de que un atacante puede haber adquirido la clave privada correspondiente del certificado.
Si un certificado no incluye controles de revocación, no se puede revocar. Emitir credenciales irrevocables constituye una infracción de las prácticas recomendadas.

Recomendación
Si el servicio no está en uso, desmantélelo. Si lo está, contacte con su CA y pida que emitan un nuevo certificado.

2 resultados

OBJETIVO	HUELLA DIGITAL SHA-256	OBSERVACIONES	SALIDA	FECHA DE ÚLTIMA OBSERVACIÓN
190.144.214.233	d5df1086ad1d754280aeb42016244b2d017eca143d6834281eeaa3cea85bdd7a02			6/10/2023 4:13:13
190.144.214.233	492daf7b137f54fcb0bdeaea793a443a2e0a5a7bbcaee9bb3d405e92f21ee206	57		7/10/2023 8:28:30

El certificado es autofirmado

-1.2 IMPACTO EN EL SCORE

Los certificados autofirmados impiden que los clientes TLS se conecten a los servidores.

Descripción

Cuando se emite un certificado, se firma con una clave privada. Los servicios accesibles al público deben tener certificados asociados con entidades de certificación (CA) públicas. Las credenciales de las entidades de certificación se almacenan en una tabla denominada almacén de confianza, integrada en los navegadores web y sistemas operativos modernos. Los certificados firmados con claves que no consten en el almacén de confianza impedirán que los clientes TLS conecten con los servidores.
Es frecuente que el software y el hardware comercial ejecuten servicios que utilizan de forma predeterminada certificados autofirmados. Si dichos servicios son accesibles al público, deben configurarse para que usen certificados emitidos por entidades de certificación conocidas. De lo contrario, se expone a los usuarios del servicio a ataques de tipo "man in the middle" (intermediario) en la Internet abierta.
Los certificados autofirmados se usan poco, pero su uso es legítimo, por ejemplo, en la protección de servicios cuyos clientes están configurados para usar la asignación de claves públicas.

Recomendación

Si el servicio no está en uso, desmantélelo. Si lo está, contacte con su CA y pida que emitan un nuevo certificado.

1 resultado

OBJETIVO	HUELLA DIGITAL SHA-256	OBSERVACIONES	SALIDA	FECHA DE ÚLTIMA OBSERVACIÓN
190.144.214.233	492daf7b137f54fcb0bdeaea7 1 93a443a2e0a5a7bbcaee9bb3 d405e92f21ee206			7/10/2023 8:28:30

A 100 CADENCIA DE APLICACIÓN DE REVISIONES

El módulo Cadencia de aplicación de revisiones analiza la rapidez con la que una empresa reacciona a las vulnerabilidades para medir las prácticas de aplicación de revisiones. Analizamos la velocidad a la que una empresa necesita hacer correcciones y aplicar revisiones en comparación con empresas similares.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Patching Cadence

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Patching Cadence

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Patching Cadence

POSITIVA

No hay Señales positivos para Patching Cadence

INFORMATIVOS

No hay Señales informativos para Patching Cadence

No se encontró ningún problema

A 100 INGENIERÍA SOCIAL

El módulo Ingeniería Social de SecurityScorecard se utiliza para determinar la susceptibilidad potencial de una organización a un ataque de ingeniería social dirigido. El módulo se nutre de datos de redes sociales y filtraciones de datos públicos, y combina métodos de análisis patentados. La puntuación de Ingeniería social es un indicador informativo calculado en función de la cantidad de indicadores que aparezcan en los sensores de recolección de SecurityScorecard.

GRAVEDAD ALTA

No hay Problemas de gravedad alta para Social Engineering

GRAVEDAD MEDIA

No hay Problemas de gravedad media para Social Engineering

GRAVEDAD BAJA

No hay Problemas de gravedad baja para Social Engineering

POSITIVA

No hay Señales positivos para Social Engineering

INFORMATIVOS

No hay Señales informativos para Social Engineering

No se encontró ningún problema

Ningún contenido (incluidos datos, calificaciones, informes, software u otra aplicación o resultado de los mismos) ya sea en todo o en parte (en su conjunto, el Contenido) puede modificarse, someterse a ingeniería inversa, reproducirse o distribuirse de ninguna forma ni por ningún medio, ni almacenarse en una base de datos o sistema de recuperación, sin el permiso previo por escrito de SecurityScorecard, Inc. (SSC). El Contenido no se utilizará para ningún propósito ilegal o no autorizado.

Ni SSC ni ningún tercero, sus directores, ejecutivos, accionistas, empleados, clientes y agentes (en su conjunto, las Partes de SSC) garantizan la exactitud, integridad, oportunidad o disponibilidad del Contenido. Las Partes de SSC no son responsables de ningún error u omisión (negligente o de otro tipo), independientemente de la causa, ni de los resultados obtenidos del uso del Contenido. El Contenido se proporciona "tal cual". LAS PARTES DE SECURITYSCORECARD RENUNCIAN A TODAS Y CADA UNA DE LAS GARANTÍAS EXPRESAS O IMPLÍCITAS, INCLUIDAS, ENTRE OTRAS, (1) GARANTÍAS DE COMERCIABILIDAD O IDONEIDAD PARA UN FIN O USO PARTICULAR, (2) GARANTÍAS DE PRECISIÓN, RESULTADOS, OPORTUNIDAD E INTEGRIDAD, (3) GARANTÍAS DE AUSENCIA DE ERRORES O DEFECTOS DE SOFTWARE (4) GARANTÍAS DE FUNCIONAMIENTO ININTERRUMPIDO DEL CONTENIDO Y (5) GARANTÍAS DE FUNCIONAMIENTO DEL CONTENIDO CON CUALQUIER CONFIGURACIÓN DE SOFTWARE O HARDWARE. En ningún caso las Partes de SSC serán responsables ante ninguna de las partes por ningún daño directo, indirecto, incidental, ejemplar, compensatorio, punitivo, especial o consecuente, ni de los costes, gastos, honorarios legales o pérdidas (incluidos, sin limitación, pérdida de beneficios o lucro cesante y costes o pérdidas de oportunidad causados por negligencia) en relación con cualquier uso del Contenido, incluso si se les informa de la posibilidad de tales daños.

LOS USUARIOS DEL CONTENIDO DEBEN HACER TODOS LOS ESFUERZOS RAZONABLES PARA MITIGAR CUALQUIER PÉRDIDA O DAÑO DE CUALQUIER TIPO (Y POR CUALQUIER CAUSA) Y NADA DE LO QUE FIGURE EN EL PRESENTE DOCUMENTO SE CONSIDERARÁ QUE EXIME O ANULA EL DEBER DE LOS USUARIOS DE MITIGAR CUALQUIER PÉRDIDA O DAÑO.

EN CUALQUIER CASO, EN LA MEDIDA PERMITIDA POR LA LEY, LA RESPONSABILIDAD AGREGADA DE LAS PARTES DE SSC RELACIONADA POR CUALQUIER RAZÓN CON EL ACCESO O EL USO DEL CONTENIDO NO SUPERARÁ LA CANTIDAD MAYOR ENTRE (A) EL IMPORTE TOTAL QUE EL USUARIO HAYA PAGADO A SSC POR LOS SERVICIOS PRESTADOS DURANTE LOS 12 MESES INMEDIATAMENTE ANTERIORES AL EVENTO QUE DA LUGAR A LA RESPONSABILIDAD, Y (B) 100 USD.

Los análisis relacionados con la seguridad, incluidas las calificaciones, y las declaraciones que figuren en el Contenido son declaraciones de opinión sobre los riesgos de seguridad relativos futuros de las entidades en la fecha en que se expresan, y no declaraciones de hechos actuales o históricos en cuanto a la seguridad de las transacciones con cualquier entidad, ni recomendaciones sobre la decisión de hacer negocios con cualquier entidad, ni avales de la exactitud de cualquiera de los datos o conclusiones o intentos de evaluar o dar fe de forma independiente de las medidas de seguridad de cualquier entidad. Las opiniones, análisis y calificaciones de SSC no deben utilizarse como sustituto de la habilidad, el buen juicio y la experiencia del usuario y de sus directivos, empleados, asesores y clientes a la hora de tomar decisiones empresariales. SSC no asume ninguna obligación de actualizar el Contenido después de su publicación en cualquier forma ni formato. Si bien SSC ha obtenido información de fuentes que considera fiables, no realiza ninguna auditoría y no asume ninguna obligación de diligencia debida ni verificación independiente de ninguna información que recibe. Los Usuarios acuerdan expresamente que (a) las calificaciones de seguridad y otras opiniones de seguridad proporcionadas a través del Contenido no reflejan, identifican ni detectan cada vulnerabilidad o problema de seguridad ni abordan ningún otro riesgo; (b) las calificaciones de seguridad y otras opiniones proporcionadas no tienen en cuenta los objetivos, situaciones o necesidades particulares de los usuarios; (c) cada calificación u otra opinión se ponderará, si corresponde, únicamente como un factor en cualquier decisión tomada por cualquier usuario o en nombre de este; y (d) los usuarios, en consecuencia, con el debido cuidado, realizarán su propio estudio y evaluación de los riesgos de hacer negocios con cualquier entidad. Si un usuario identifica alguno en el Contenido, le invitamos a compartir esa información con nosotros enviándonos un correo electrónico a support@securityscorecard.io.